IdPメタデータテンプレート

IdPメタデータの作成サンプル（★）

以下のメタデータテンプレートはこちらからダウンロードできます。
※実習セミナーでは、/root/GETFILE/からコピーしたものを利用するので、ダウンロードは行いません。
⇒IdPメタデータテンプレート

実習セミナー

スコープ（shibmd:Scope）は、「**nii.ac.jp**」とします。（2カ所）
OrganizationDisplayNameの「XX」部分を割り振られた番号に変更します。

例）1番を割り振られた場合
・ホスト名：
ex-idp-test01.gakunin.nii.ac.jp
・mdui:DisplayName、OrganizationDisplayName：
en) Ex-IdP-Test01
ja) 実習セミナーIdPテスト01

尚、使用するテンプレートメタデータでは下記の要素を省略していますので、当該項目の修正（追加）の必要はありません。
・mdui:UIInfo
→ mdui:Logo、mdui:InformationURL（ja/en）、mdui:PrivacyStatementURL（ja/en）
・mdui:DiscoHints
→ mdui:IPHint、mdui:DomainHint、mdui:GeolocationHint

ホスト名や証明書は、構築したIdPの情報に変更してください。

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://IdP-HostName/idp/shibboleth">
                                                                                ↑ ホスト名
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:mace:shibboleth:1.0 urn:oasis:names:tc:SAML:
2.0:protocol">
    <Extensions>
      <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" regexp="false">SCOPE</shibmd:Scope>
                                                                                ↑ 構築したIdPのスコープ
      <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
        <mdui:DisplayName xml:lang="ja">実習セミナーIdPテストXX</mdui:DisplayName>
        <mdui:DisplayName xml:lang="en">Ex-IdP-TestXX</mdui:DisplayName>
                                        ↑ IdP名称（英/日）
                                         DSに表示されます。※学認DSでは、OrganizationDisplayNameよりも優先されます。
                                         登録先DS内で一意になるようにして下さい。
                                         同じ名前があると、DSでIdP選択が行えなくなります。
        <mdui:Logo height="50" width="50">https://IdP-HostName/logo/logo.jpg</mdui:Logo>
                                             ↑ ロゴ画像URL
                                              学認DSのIdPリストや地図表示でロゴが表示されます。
        <mdui:InformationURL xml:lang="ja">https://IdP-HostName/jp/</mdui:InformationURL>
        <mdui:InformationURL xml:lang="en">https://IdP-HostName/en/</mdui:InformationURL>
                                             ↑ IdP情報URL（英/日）
        <mdui:PrivacyStatementURL xml:lang="ja">https://IdP-HostName/jp/privacy</mdui:PrivacyStatementURL>
        <mdui:PrivacyStatementURL xml:lang="en">https://IdP-HostName/en/privacy</mdui:PrivacyStatementURL>
                                                  ↑ プライバシーステートメントURL（英/日）
        <mdui:Keywords xml:lang="en">category:location:kanto category:organizationType:university</mdui:Keywords>
                                        ↑ 地域                    ↑ IdPカテゴリ
                                         ※共に学認DSのIdPリスト表示で使用されます。
                                           地域は、IdPリスト内のカテゴリ分け（北海道、東北、関東...など）に使います。
                                           IdPカテゴリは、IdPリストの表示フィルタリング（大学、短大、高専...など）で使います。
      </mdui:UIInfo>
      <mdui:DiscoHints xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
        <mdui:IPHint>192.168.0.0/16</mdui:IPHint>
                    ↑ 学認DSのヒント機能に使われるネットワークアドレスです。
                      ※ネットワークマスク設定が必要です。
        <mdui:DomainHint>nii.ac.jp</mdui:DomainHint>
                     ↑ 学認DSのヒント機能に使われるドメインです。
        <mdui:GeolocationHint>geo:35.6924668,139.75810019999994</mdui:GeolocationHint>
                                       ↑ 学認DSのヒント機能や地図表示に使われる緯度経度の座標です。
                                         ※先頭に「geo:」を付けます。
      </mdui:DiscoHints>
    </Extensions>
    <KeyDescriptor>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
```

```
MIIFITCCBAmgAwIBAgIIBpAaVBrt6kMwDQYJKoZIhvcNAQEFBQAwfTELMAkGA1UE
BhMCSlAxETAPBgNVBAcTCEFjYWRlbWUyMSowKAYDVQQKEyFOYXRpb25hbCBJbnN0
aXR1dGUgb2YgSW5mb3JtYXRpY3MxDTALBgNVBAsTBFVQS0kxIDAeBgNVBAsTF05J
（中略）
kBFfvNBdrux4CkIsKhpYQXCAIEuy12CFZUXEtHB5XxeBkntbs2lfP/rWbg2J1Ige
zZc6shCn3VdrL2douVFjaAXlc8zwys/KIpLzNSxOOGwJdKxFTaIzH/emcqKj93Jd
DC1rrFMhoPE=
↑ 設定した証明書に変更（/opt/shibboleth-idp/credentials/server.crt）
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
    <SingleSignOnService Location="https://IdP-HostName/idp/profile/Shibboleth/SSO" Binding="urn:mace:shibboleth:1.0:profiles:
AuthnRequest"/>
                                          ↑ ホスト名
    <SingleSignOnService Location="https://IdP-HostName/idp/profile/SAML2/POST/SSO" Binding="urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-POST"/>
                                          ↑ ホスト名
    <SingleSignOnService Location="https://IdP-HostName/idp/profile/SAML2/Redirect/SSO" Binding="urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect"/>
                                          ↑ ホスト名
  </IDPSSODescriptor>
  <AttributeAuthorityDescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol"
>
    <Extensions>
      <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" regexp="false">SCOPE</shibmd:Scope>
                                                                                  ↑ 構築したIdPのスコープ
    </Extensions>
    <KeyDescriptor>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
MIIFITCCBAmgAwIBAgIIBpAaVBrt6kMwDQYJKoZIhvcNAQEFBQAwfTELMAkGA1UE
BhMCSlAxETAPBgNVBAcTCEFjYWRlbWUyMSowKAYDVQQKEyFOYXRpb25hbCBJbnN0
aXR1dGUgb2YgSW5mb3JtYXRpY3MxDTALBgNVBAsTBFVQS0kxIDAeBgNVBAsTF05J
（中略）
kBFfvNBdrux4CkIsKhpYQXCAIEuy12CFZUXEtHB5XxeBkntbs2lfP/rWbg2J1Ige
zZc6shCn3VdrL2douVFjaAXlc8zwys/KIpLzNSxOOGwJdKxFTaIzH/emcqKj93Jd
DC1rrFMhoPE=
↑ 設定した証明書に変更（/opt/shibboleth-idp/credentials/server.crt）
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <AttributeService Location="https://IdP-HostName:8443/idp/profile/SAML1/SOAP/AttributeQuery" Binding="urn:oasis:names:tc:SAML:1.0:
bindings:SOAP-binding"/>
                                        ↑ ホスト名
    <AttributeService Location="https://IdP-HostName:8443/idp/profile/SAML2/SOAP/AttributeQuery" Binding="urn:oasis:names:tc:SAML:2.0:
bindings:SOAP"/>
                                        ↑ ホスト名
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
  </AttributeAuthorityDescriptor>
  <Organization>
    <OrganizationName xml:lang="en">Training Seminar University</OrganizationName>
    <OrganizationName xml:lang="ja">実習セミナー大学</OrganizationName>
                                      ↑ 機関名称（英/日）
    <OrganizationDisplayName xml:lang="en">Ex-IdP-TestXX</OrganizationDisplayName>
    <OrganizationDisplayName xml:lang="ja">実習セミナーIdPテストXX</OrganizationDisplayName>
                                          ↑ IdP名称（英/日）
                                            DSに表示されます。※学認DSでは、mdui:DisplayNameが優先されます。
                                            登録先DS内で一意になるようにして下さい。
                                            同じ名前があると、DSでIdP選択が行えなくなります。
    <OrganizationURL xml:lang="en">http://YourHomePage/</OrganizationURL>
                                        ↑ 機関情報URL（英/日）
  </Organization>
  <ContactPerson contactType="technical">
                                ↑ 連絡先ポジションを以下から選択
                                [technical, support, administrative, billing, other]
    <GivenName>Your GivenName</GivenName>
                    ↑ 連絡先名（名）
    <SurName>Your SurName</SurName>
                  ↑ 連絡先名（姓）
    <EmailAddress>mailto:admin@example.org</EmailAddress>
```

```
                                ↑ 連絡先のe-mailアドレス
                                （メタデータは公開されるのでalias名などを推奨：学認技術運用基準4.4項参照）
  </ContactPerson>
</EntityDescriptor>
```

※端末のサイズによっては表記がずれる可能性がございます。画面を広くしてご覧ください。

上記のように、IdPメタデータは大きく<IDPSSODescriptor>の部分と<AttributeAuthorityDescriptor>の部分に分かれます。前者が通常のSSOで使用される部分で、後者はバックチャネル（8443番ポート）での通信で使われる部分です。このため証明書情報を2か所に書いていただく必要がありますが、本技術ガイドに沿った構築では同じものを記載いただきます。

※ 証明書は複数指定できます。例えば証明書を更新する場合などは一時的に古い証明書と新しい証明書の両方を並行運用したい場合があるでしょう。複数の証明書 を記載する場合は<KeyDescriptor>部分を繰り返してください（下記参照）。2カ所ありますので両方変更することを忘れないでください。

```
    <KeyDescriptor>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>■１枚目</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <KeyDescriptor>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>■２枚目</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
```